CCNA Study Guide

Alexander

June 12, 2024

1. Network Fundamentals (20%)
2. Network Access (20%)
3. IP Connectivity (25%)
4. IP Services (10%)
5. Security Fundamentals (15%)
6. Automation and Programmability (10%)

Network Fundamentals

- **Explain the role and function of network components**

  Routers forward packets between computer networks (LANs and WANs), and use IP addresses to determine where a packet should go. Routers remove data-link headers and trailers, analyze packet information, and then re-encapsulate the data with a new data-link frame before transmission. Routers compare destination IPs, found inside packet headers, to routes in routing tables before forwarding packets. Routing tables get their routes from static routes, dynamic routing protocols, and source headers fields found in packets recieved on local interfaces. Routers can perform many different actions: implementing QoS tools, permiting/denying packets with ACLs, performing firewall functions, advertising BSSs, and more.

  Switches forward PDUs at layer 2 within the same network segment. Switches place new source MAC addresses, found in the header fields, into a table. This MAC-address table helps the switch make forwarding decisions. Switch ports divide collision domains; unlike router ports, which divide broadcast domains. Switches can divide broadcast domains by using VLANs, but cannot route between subnets. Switches can perform a variety of security tasks as well like: port security, DAI, DHCP snooping. L3 switches can perform both switching and routing functions.

Firewalls sit in the path that packets take through the network. They permit/deny traffic much like an ACL would do on a router. Firewalls are capable of watching application-layer flows with AVC, performing webpage verification on URIs, and retaining state. IPSs can compare packet flows to exploit signatures, log events, and can discard/redirct packets.

An AP serves as a single point of contact for every device that wants to use a BSS. An AP uses a unique BSSID that is based on the AP's own radio MAC address. APs are often connected to a DS that uplinks to a wired network.

- **Describe characteristics of network topology architectures**
- **Compare physical interface and cabling types**
- **Identify interface and cable issues (collisions, error, mismatch duplex, and/or speed)**
- **Compare TCP to UDP**
- **Configure and verify IPv4 addressing and subnetting**

  configure: Router(config-if)# ip address <ip_address> <subnet_mask>

  verify: Router# show ip interface brief
- **Describe private IPv4 addressing**
- **Configure and verify IPv6 address types**

  configure: Router(config-if)# ipv6 address <IPv6_address>/<prefix_length>

  verify: Router# show ipv6 interface brief
- **Describe IPv6 addressing and prefix**
- **Verify IP parameters for Client OS**
- **Describe wireless principles**
- **Explain virtualization fundamentals (server virtualization, containers, and VRFs)**
- **Describe switching concepts**

Network Access

- **Configure and verify VLANs (normal range 0-1005) spanning multiple switches**

  1. create vlans, 2. port operation, 3. apply vlans
Switch(config)# vlan <vlan-id>
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan <vlan-id>

verify: defined/active VLANs, VTP, access ports(data and voice)
Switch# show vlan [brief]
Switch# show interface interface_type interface_number [brief]
Switch# show interfaces status
Switch# show run

- **Configure and verify interswitch connectivity**

  1. operational mode, 2. allowed vlans, 3. encapsulation standard, 4. native vlan
  Switch(config-if)# switchport mode trunk
  Switch(config-if)# switchport trunk allowed vlan <10,20,30>
  Switch(config-if)# switchport tunk encapsulation <dot1q/isl>
  Switch(config-if)# switchport trunk native vlan <vlan-id>

  verify: VLANs, native VLAN, VTP, DTP, operational mode
  Switch# show interface trunk
  Switch# show interfaces switchport
  Switch# show interface interface_name interface_number

- **Configure and verify L2 discovery protocols (CDP/LLDP)**

  CDP: multicast address 0100.0ccc.cccc
  Switch(config-if)# cdp enable
  Switch(config)# cdp run
  Switch(config)# cdp timer seconds
  Switch(config)# cdp holdtime seconds

  verify↓
  Switch# show cdp neighbors <interface>
  Switch# show cdp neighbors detail
  Switch# show cdp entry name
  Switch# show cdp interface <interface>
  Switch# show cdp
  Switch# show cdp traffic

  LLDP(802.1AB): multicast address 0180.c200.000e
  Switch(config)# lldp run
  Switch(config-if)# lldp transmit
  Switch(config-if)# lldp receive
  Switch(config)# lldp timer seconds
  Switch(config)# lldp holdtime seconds

- verify↓
  Switch# show lldp
  Switch# show lldp traffic
  Switch# show lldp interface
  Switch# show lldp neighbors

Switch# show lldp neighbors detail
Switch# show lldp entry name

- **Configure and verify (L2/L3) EtherChannel (LACP)**

  Manual Configuration↓
  Switch(config-if-range)# channel-group 1 mode on
  Switch(config)# port-channel load-balance method (src. and or dest. MACs/IPs/port numbers)

  Dynamic Congifuration↓
  Switch(config-if-range)# channel-group 1 mode <desirable/auto>(PAgP)
  Switch(config-if-range)# channel-group 1 mode <active/passive>(LACP)

  verify: speed, duplex, operational mode, VLANs, STP
  Switch# show etherchannel summary
  Switch# show interfaces status

  L3 Etherchannel configuration is similar to L2 configuration:
  1. each physical port needs to be a routed port (no switchport command)
  2. also the actuall channel needs to be a routed port with an IP and mask

- **Interpret basic operations of Rapid PVST+ Spanning Tree Protocol**

- **Describe Cisco Wireless Architectures and AP modes**

- **Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)**

- **Describe network device management access (Telnet, SSH, HTTP, HTTPS, console, TACACS+/RADIUS, and cloud managed)**

- **Interpret the wireless LAN GUI configuration for client connectivity, such as WLAN creation, security settings, QoS profiles, and advanced settings**

IP Connectivity

- **Interpret the compnents of routing table**

- **Determine how a router makes a forwarding decision by default**

- **Configure and verify IPv4 and IPv6 static routing**
  NOTE: using the link-local address as the next hop address is ambigious you must include the outgoing-interface beforehand
  NOTE: IOS allows you to configure the ipv6 route command using only the outgoing-interface parameter, without listing a next-hop address. The

router will accept the command; however, if that outgoing interface happens to be an Ethernet interface, the router cannot successfully forward IPv6 packets using the route.

Default routes are used when a packet's destination address does not match any routes, but you do not want the router to discard a packet that it otherwise would.
Router(config)# ip route 0.0.0.0 0.0.0.0 <interface>
Router(config)# ipv6 router ::/0 <interface>

Network routes define a route to an entire subnet.
Router(config)# ip route 172.16.2.0 255.255.255.0 s0/0/0
Router(config)# ip route 172.16.3.0 255.255.255.0 172.16.5.3
Router(config)# ipv6 route 2001:db8:1111:2::/64 s0/0/0

Host routes match a single IP. An engineer may want to route most packets to some subnet through one route but packets destined for a specific host through another route.
Router(config)# ip route 10.1.1.9 255.255.255.255 10.9.9.9
Router(config)# ipv6 router 2001:db8:1111:2::22/128 s0/0/0 fe80::ff:fe00:2

Floating static routes are used when when a primary route fails.
Router(config)# ip route 172.16.2.0 255.255.255.0 172.16.5.3 130
Router(config)# ipv6 route 2001:db8:1::/64 2001:db8:2::1 200

- **Configure and verify single area OSPFv2**

  Direct↓
  Router(config)# ospf process <1-65535>
  Router(config-router)# router-id X.X.X.X (OPTIONAL) Router(config-router)# network <IP_address><wildcard>area <area_id>

  Indirect↓
  Router(config-if)# ip ospf process <1-65535><area_id>
  Router(config-if)# ip ospf network [type] (OPTIONAL)

  Passive interfaces do not send Hellos but information about the connected subnet will still be advertised elsewhere.
  Router(config-router)# passive-interface <interface>

  OSPF default routes work like normal default routes, but can be advertised via OSPF
  Router(config-router)# default-information originate

  OSPF cost = reference / bandwidth
  Router(config-if)# ip ospf cost cost (explicitly set cost value 1-65535)
  Router(config-router)# auto-cost reference (alters the cost calulation)
  Router(config-if)# speed 100
  (affects the actual speed at which data is transmitted an recieved on the

interface)
Router(config-if)# bandwidth 10000
(in scenarios where the actual bandwidth of the interface differs from the default assumption made by the routing protocol)
Router(config-if)# clock
(configured on the DCE end of a serial link to provide clocking for the line)

OSPF route summarization involves aggregating multiple contiguous network addresses into a single summary route advert.
NOTE: Route summarization should be done at the netwrok boundary to avoid potential routing issues. Also, make sure that summarized routes cover all the individual routes being summarized.
Router(config-router)# area 0 range <IP_address><subnet_mask>

Routing Black Holes:
A routing black hole occurs when a router receives traffic for a destination network but does not have a valid route to forward that traffic. This can happen due to various reasons, including misconfigured routes, unreachable next hops, or route summarization that omits specific routes. When a router encounters a routing black hole, it frops the packets, resulting in loss of connectivity to the affected destination.

Suboptimal Routing Decisions:
Suboptimal routing decisions refer to situations where routers select paths that are not the most efficient or optimal routes to reach a destination. This can occur due to factos such as unequal cost load balancing, asymmetric routing, or inefficient routing protocols. Suboptimal routing decisions can lead to increased latency, congestion, and subpar network performance.

verify: MTU, areas, network types, timers, neighbor states/roles, reference bandwidth, authentication
Router(config)# show run (config)
Router(config)# show ip protocols (config)

Router(config)# show ip ospf interface (enabled interfaces)
Router(config)# show ip ospf interface <interface>(enabled interfaces)
Router(config)# show ip ospf interface brief (enabled interfaces)

Router(config)# show ip ospf neighbor (neighbors) Router(config)# show ip ospf neighbor <interface>(neighbors)

Router(config)# show ip ospf database (lsdb)

Router(config)# show ip ospf rib (rib)

Router(config)# show ip route (routes)
Router(config)# show ip route ospf (routes)
Router(config)# show ip route subnet mask (routes)
Router(config)# show ip route — section subnet (route)

- **Describe the purpose, functions, and concepts of first hop redundancy protocols**

IP Services

- **Configure and verify inside source NAT using static and pools**

  Static NAT
  Router(config-if)# ip nat inside
  Router(config-if)# ip nat outside
  Router(config)# ip nat inside source static <insidelocal><insidelocal>

  Dynamic NAT
  Router(config)# ip nat pool mypool 203.0.113.20 203.0.113.30 netmask 255.255.255.0
  Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
  Router(config)# ip nat inside source list 1 pool mypool

  verify: interfaces, address ranges, acl, hit/misses, routes to destinations↓
  R1# show access-lists
  R1# show ip nat translations [verbose]
  R1# show ip nat statistics
  R1# show ip route
  R1# show run
  R1# show interfaces <interface>

- **Configure and verify NTP operating in a client and server mode**

  software clock↓
  Router# clock set hh:mm:ss day—month month—day year

  hardware clock↓
  Router# calendar set hh:mm:ss day—month day—month year

  timezones↓
  Router(config)# clock timezone name hours-offset [minutes-offset]

  daylight savings↓
  Router(config)# clock summer-time recurring name start end [offset]

NTP uses UTC time standard to sync network devices
R1(config)# ntp update-calendar
R1(config)# interface loopback0
R1(config-if)# ip address 10.1.1.1 255.255.255.255
R1(config)# ntp source loopback 0
R1(config)# ntp master <1-15>
R2(config)# ntp server 10.1.1.1 [prefer]
R2(config)# ntp peer 10.0.23.3
R3(config)# ntp peer 10.0.23.2
R3(config)# ntp authenticate
R3(config)# ntp authentication-key key-number md5 key
R3(config)# ntp trusted-key key-number
R3(config)# ntp server 10.1.1.1 key key-number

verify ↓
Router# show ntp associations
(* sys.peer, # selected, + candidate, - outlyer, x falseticker, configured)
Router# show ntp status

- **Explain the role of DHCP and DNS within the network**

- **Explain the function of SNMP in network operations**

- **Describe the use of syslog features including facilities and levels**

- **Configure and verify DHCP client and relay**

  DHCP relay is used to help move DHCP messages in/out of a segment
  Router(config-if)# ip helper-address 192.168.1.100

  show commands ↓
  show ip dhcp binding
  show ip dhcp pool
  show ip dhcp server statistics
  show ip dhcp relay
  ipconfig or ifconfig (verify clients DHCP information)

- **Explain the forwarding per-hop behavior (PHB) for QoS, such as classification, marking, queuing, congestion, policing, and shaping**

- **Configure network devices for remote access using SSH**

  1. enable SSH 2. create user accounts 3. set parameters 4. access control (OPTIONAL)
  Router(config)# crypto key generate rsa
  Router(config)# username <username>priviledge 15 secret <pass>
  Router(config)# ip ssh version 2
  Router(config)# ip ssh time-out 120
  Router(config)# ip ssh authentication-retries 3

verify by attempting a remote login
Router# show run — include ssh
Router# show ip ssh

- **Describe the capabilities and functions of TFTP/FTP in the network**

Security Fundamentals

- **Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)**
- **Describe security program elements (user awareness, training, and physical access control)**
- **Configure and verify device access control using local passwords**

  configure↓ Router(config)# service password-encryption

  Router(config)# enable secret <password>

  Router(config)# line console 0
  Router(config-line)# password <password>
  Router(config-line)# login

  Router(config)# line vty 0 15
  Router(config-line)# password <password>
  Router(config-line)# login

  verify↓ Router# show run — include enable secret Router# show run — include line console 0 Router# show run — include line vty 0 15

- **Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)**
- **Describe IPsec remote access and site-to-site VPNs**
- **Configure and verify access control lists**

  Standard ACLs match source IP addresses only.
  R1(config)# access-list 1 deny [host] 192.168.1.233 [log]

  Extended ACLs have more matching parameters.
  R1(config)# access-list 101 permit tcp 172.16.1.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21

Named ACLs have a subconfiguration mode with sequence numbers
Router(config)# ip access-list extended barney
Router(config-ext-nacl)# permit tcp host 10.1.1.2 eq www any
Router(config-ext-nacl)# interface serial1
Router(config-if)# ip access-gorup barney out

verify:
Place standard ACLs as close to the destination as possible.
Place extended ACLs as close to the source as possible.
Disable an ACL before altering the ACEs.

NOTE: helpful arithmetic ↓
subnet = host address &(binary and) mask
wildcard mask = limited broadcast address - subnet mask
subnet(highend) = subnet(lowend) + wildcard
0d → 0b ↓
1. continue to divide by 2
2. each division set aside the remainder
3. once the quotient is 0, merge the remainders in reverse order 0x → 0d ↓
1. separate the digits and convert them to decimal digits
2. multiply each digit by the respective power of 16
3. add them
0d → 0x ↓
1. identify the largest power of 16 less than the decimal number
2. continue to divide the remainders by the largest power of 16 setting the quotient aside
3. merge remainders and convert them individually

- **Configure and verify Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)**

DHCP snooping is used to prevent spurious DHCP servers
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan <vlan_id>
Switch(config-if)# ip dhcp snooping trust verify↓
Switch# show ip dhcp snooping
Switch# show ip dhcp snooping binding

dynamic ARP inspection is used prevent ARP spoofing/poisoning
Switch(config)# ip arp inspection
Switch(config)# ip arp inspection vlan <vlan_id>
Switch(config-if)# ip arp inspection trust verify↓ Switch# show ip arp inspection
Switch# show ip arp inspection statistics

port security is used to keep unauthorized devices from accessing the network
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum <value>
Switch(config-if)# switchport port-security violation shutdown — restrict — protect
verify↓ Switch# show port-security interface <interface>
Switch# show port-security [address]

- **Compare authentication, authorization, and accounting concepts**
- **Describe wireless security protocols (WPA, WPA2, and WPA3)**
- **Configure and verify WLAN within the GUI using WPA2 PSK**

1. Access the GUI

2. Login

3. Navigate to WLAN Settings

4. Create a New WLAN Profile

5. Configure WLAN Settings: SSID, security settings, pre-shared key, encryption, etc.

6. Apply and Save Changes

7. Verify WLAN Configuration

8. Test Connectivity

Automation and Programmability

- **Explain how automation impacts network management**
- **Compare traditional networks with controller-based networking**
- **Describe controller-based, software defined architecture (overlay, underlay, and fabric)**
- **Explain AI (generative and predictive) and machine learning in network operations**
- **Describe characteristics of REST-based APIs (authentication types, CRUD, HTTP verbs, and data encoding)**
- **Recognize the capabilities of configuration management mechanisms, such as Ansible and Terraform**
- **Recognize components of JSON-encoded data**